

### REMARKS

This amendment is in response to the Office Action mailed April 7, 2006. In the amendment, claims 1, 6 and 17 have been amended, and claims 1-12 and 17 remain pending in the application. Reconsideration of the pending claims in light of the amendment and the following remarks is respectfully requested.

These amendments add no new matter. The features of public key certificates having basic and extended areas, respectively identifying first and second signature algorithms in those areas, and generating signatures by respectively applying the first and second signature algorithms to information in both the basic and extended areas are variously described in Applicant's specification. This description includes but is not necessarily limited to the depictions of certificates in FIGs. 11-13, the following flow diagrams, and the related descriptions of those figures.

Claims 1-3, 6, 8, 9 and 12-17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 6,157,721 to Shear ("Shear") in view of Whittle, "Public Key Authentication Framework: Tutorial," First Principles Consulting, 2 June 1996 ("Whittle") and Chokhani, "Comment on RFC 2527," The Internet Society, March 1999 ("Chokhani"). This rejection is traversed.

Independent claim 1 has been amended and now recites: *[a] public key certificate issuing system comprising:*

*a certificate authority for issuing a public key certificate of an entity which uses said public key certificate; and*

*a registration authority for sending a public key certificate issuing request received from an entity under control to said certificate authority;*

*said certificate authority being constituted by a plurality of certificate authorities each executing a different signature algorithm, transferring a public key certificate between said plurality of certificate authorities in response to said public key certificate issuing request received from said registration authority, attaching a digital signature on message data constituting said public key certificate in accordance with said different signature algorithm at*

*each certificate authority, and issuing a multi-signed public key certificate storing a plurality of signatures based on different signature algorithms,*

*wherein said multi-signed public key certificate includes at least a basic area and an extended area, the basic area storing information identifying a first different signature algorithm executed by a first of the plurality of certificate authorities, and the extended area storing information identifying a second different signature algorithm executed by a second of the plurality of certificate authorities, and*

*wherein first and second signatures are generated by respectively applying the first and second different signature algorithms to information in both the basic area and the extended area.*

These claimed features are neither disclosed nor suggested by Shear, Whittle, and Chakhani, whether taken alone or in combination.

Shear discloses techniques for the protection of secure computing environments, specifically through the certification of what are referred to as "load modules" (54). As described in Shear:

These load modules--which can be transmitted from remote locations within secure cryptographic wrappers or "containers"--are used to perform the basic operations of the "virtual distribution environment." Load modules may contain algorithms, data, cryptographic keys, shared secrets, and/or other information that permits a load module to interact with other system components (e.g., other load modules and/or computer programs operating in the same or different protected processing environment). For a load module to operate and interact as intended, it must execute without unauthorized modification and its contents may need to be protected from disclosure.

(Shear, at 3:24-35).

The Examiner apparently relies upon the association between such load modules and a "verifying authority" in alleging that Shear discloses a certificate authority for issuing a public key certificate of an entity which uses the public key certificate, wherein the certificate authority is constituted by plural certificate authorities each executing a different signature algorithm; transferring a public key certificate between said plurality of certificate authorities in response to said public key certificate request; attaching a digital signature on message data constituting said public key certificate in accordance with the different signature algorithms of each certificate

authority; and issuing a multi-signed public key certificate storing a plurality of signatures based on the different signature algorithms. (Office Action, at pp. 3-4).

In that regard, the Examiner refers to FIG. 7 and other passages. FIG. 7 the related description of the load module indicates that multiple digital signatures can be created for a given load module. A verification authority is also generally described for certifying load modules. (e.g., Shear at 10:32-53). However, there is no apparent description of a registration authority and a certificate authority constituted by multiple certificate authorities each executing a different signature algorithm, with the registration authority sending a public key certificate issuing request to the certificate authority.

Nor, as the Examiner states in the Action, does Shear disclose a public key certificate that includes at least a basic area and an extended area. (Office Action, at p. 4). Applicant also notes that amended claim 1 is further distinguished from Shear, in that the claim recites that *“the basic area stor[es] information identifying a first different signature algorithm executed by a first of the plurality of certificate authorities, and the extended area stor[es] information identifying a second different signature algorithm executed by a second of the plurality of certificate authorities,”* and *“wherein first and second signatures are generated by respectively applying the first and second different signature algorithms to information in both the basic area and the extended area.”*

Whittle and Chokhani do not remedy the deficiencies of Shear. Although Whittle generally refers to a registration authority (Organizational Registration Authority, p. 8 of Whittle), there is no apparent description of a corresponding certificate authority constituted by a plurality of certificate authorities each executing a different signature algorithm, as claimed by Applicant. Additionally, Whittle offers no disclosure or suggestion of any of the above-described features related to the basic and extended areas of the certificate.

Chokhani is a policy and certification practices framework memorandum that makes reference to a Certificate Policies Extension and a Policy Mappings Extension (Whittle, §§ 3.3.1-2, pp. 5-7). Neither of these extensions discloses the above-described features related to the basic and extended areas, different signature algorithms, and corresponding signatures. The Policy Mappings extension allows for an indication that certain policies in a given CA's domain can be considered equivalent to certain other policies in another CA's domain. It is unclear,

how, if at all, this feature relates even generally to the provision of a basic and an extended area in the digital certificate as claimed by Applicant. In any event, this feature of Chokhani in no way discloses or suggests “*the basic area storing information identifying a first different signature algorithm executed by a first of the plurality of certificate authorities, and the extended area storing information identifying a second different signature algorithm executed by a second of the plurality of certificate authorities,*” and “*wherein first and second signatures are generated by respectively applying the first and second different signature algorithms to information in both the basic area and the extended area,*” as recited in amended claim 1.

The Certificate Policies extension allows an indication of what policies are to be used, as well as whether they are “critical”. For example, electronic mail applications and Web servers might be configured to require the General-Purpose policy and an airline’s financial applications might be configured to require the Commercial-Grade policy. (Chokhani, at p. 6). The critical field allows a designation that the certificate is restricted to an identified policy, and is intended to protect the certification authority against damage claims by a relying party who uses the certificate in an inappropriate matter. (*Id.*). Again, this feature offers no disclosure or suggestion of the above-described features. There is no mention of even having separate areas for identifying different signature algorithms. It follows that there is clearly no disclosure of identifying a first different signature algorithm in the basic area, identifying a second different signature algorithm in the extended area, or generating first and second signatures by respectively applying the first and second different signature algorithms to information in both the basic and extended areas.

Since even the proposed combination of Shear, Whittle, and Chokhani would still fail to yield the claimed invention, Applicant submits that a *prima facie* case of obviousness for claim 1 has not been presented, notwithstanding the impropriety of seeking to combine the references in the offered fashion.

For reasons similar to those provided regarding claim 1, independent claims 6 and 17 are also neither disclosed nor suggested by Shear, Whittle, and/or Chokhani, whether taken alone or in any combination. Dependent claims 2-4 and 16-21 respectively incorporate the distinct features of the independent claims and thus are not disclosed by the relied-upon references for their inclusion of such features as well as their separately recited, distinct features.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 1-3, 6, 8, 9 and 12-17 under 35 U.S.C. § 103(a) as being unpatentable over Shear in view of Whittle and Chokhani.

Claims 4, 5, 10 and 11 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Shear in view of Whittle and Chokhani, and further in view of Levi et al., "A Multiple Signature Based Certificate Verification Scheme," Proceedings of BAS'98, The Third Symposium on Computer Networks, June 1998 ("Levi"). This rejection is traversed.

Each of these claims depends directly or indirectly from the above-mentioned independent claims, and thus incorporate the features recited therein. As described, even the combination of Shear, Whittle, and Chokhani fails to disclose or suggest the features recited in the independent claims, such as *"said certificate authority being constituted by a plurality of certificate authorities each executing a different signature algorithm,"* and *"wherein said multi-signed public key certificate includes at least a basic area and an extended area, the basic area storing information identifying a first different signature algorithm executed by a first of the plurality of certificate authorities, and the extended area storing information identifying a second different signature algorithm executed by a second of the plurality of certificate authorities,"* and *"wherein first and second signatures are generated by respectively applying the first and second different signature algorithms to information in both the basic area and the extended area."*

Levi does not remedy the deficiencies of the other relied-upon references. Levi discloses a multiple signature based certificate verification scheme that involves nested signatures. As stated, a nested signature is a signature over another signature and is used to verify the subject signature without using the public key of the issuer of the subject signature. (Levi, Abstract). There is no disclosure or suggestion of the features of provision of plural certificate authorities each executing different signature algorithms, separate basic and extended areas that respectively identify first and second different signature algorithms executed by those certificate authorities, or generating the first and second signatures by applying the different signature algorithms to information in both the basic and extended areas, all features recited in the independent claims.

Applicant also objects to the taking of official notice with regard to claims 5 and 11. Applicant submits that the provision of a flag indicating the presence of the additional signature

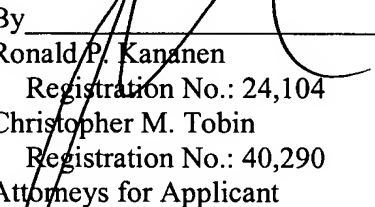
is feature is neither disclosed nor suggested by any of the relied upon references, particularly in the context of what is claimed by Applicant.

Accordingly, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 4, 5, 10, and 11 under 35 U.S.C. § 103(a) as being unpatentable over Shear in view of Whittle and Chokhani, and further in view of Levi.

For the foregoing reasons, reconsideration and allowance of the claims which remain in the application are solicited. If any further issues remain, the Examiner is invited to telephone the undersigned to resolve them.

Dated:

Respectfully submitted,

By   
Ronald P. Kananen  
Registration No.: 24,104  
Christopher M. Tobin  
Registration No.: 40,290  
Attorneys for Applicant

**RADER, FISHMAN & GRAUER, PLLC**  
Lion Building  
1233 20<sup>th</sup> Street, N.W., Suite 501  
Washington, D.C. 20036  
Tel: (202) 955-3750  
Fax: (202) 955-3751  
Customer No. 23353